

REMARKS

Introduction

This Reply is in response to the Office Action of June 8, 2010. Reconsideration of this application in view of the following remarks is respectfully requested.

Subject Matter Indicated to be Allowable

Claims 1-12, 18, and 19 were allowed. Applicants hereby reserve the right to pursue the subject matter of these claims during subsequent prosecution should the present Reply not be considered to place this application in condition for allowance.

The §112 Rejections

Claims 13-17 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In particular, it was suggested that the preamble of claim 13 (which states that the method of claim 13 relates to signing and encrypting a message) is not appropriate because the steps set forth in the body of claim 13 are purportedly not related to signing or encrypting a message M. This characterization of the steps of the body of claim 13 is not

correct. For example, the step of computing the commitment to the secret value and the corresponding decommitment that is set forth in the body of claim 13 is related to signing the message. (See, for example, decommitment computation step 80 of FIG. 6 which relate to signing the message, as described in the paragraph of applicant's specification that bridges pages 28 and 29.) In any event, applicants have removed the preamble language to expedite prosecution.

It was also suggested that the phrases "commitment" and "decommitment" are not clearly defined in the specification. Applicant disagrees. These terms are well understood cryptographic terms and, in the context of applicant's invention, are described in a detailed and mathematically rigorous fashion throughout applicant's specification.

For example, applicant describes at page 29, lines 13-19 that a sender may use a selected secret value r , the sender's IBE public key ID_A , and the hash function H_0 to calculate a commitment j to the secret value r (step 76 of FIG. 6). FIG. 6 provides an example of an equation that may be used for calculating a commitment j . The exponential notation used in FIG. 6 and the other FIGS. signifies multiplication of a point on the elliptic curve E by an integer.

Applicant describes at page 29, lines 20-25 that a user may use hash function H_1 to calculate a digest h from the

concatenation of j and message M (step 78 of FIG. 6). A decommitment v corresponding to the commitment j can be calculated using the IBE private key of the sender's private key SK_A and the values of r and h (step 80 of FIG. 6).

As evidence by the exemplary equations provided for calculating both commitments and corresponding decommitments, applicant's specification clearly defines the "commitment" and "decommitment" of claim 13. Claim 13 therefore satisfies the requirements of §112.

In view of these remarks, the 35 U.S.C. §112 rejections of claims 13-17 should be withdrawn.

The Prior Art Rejections

In the Office Action, claims 13-17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gentry et al. U.S. Patent No. 7,353,395 in view of Deng et al. U.S. Patent No. 6,910,129. These rejections are respectfully traversed.

Claims 13-17

Nothing like the arrangement of claim 13 is shown or suggested by Gentry and Deng.

In the rejection of claim 13, it was suggested that Gentry's public key P_A is equivalent to the claimed commitment, that Gentry's non-interactive shared secret S_{AB} is equivalent to

the claimed secret value, and that Gentry's private key S_A is equivalent to the claimed decommitment.

Gentry's public key P_A is not a commitment to a secret value and Gentry's private key S_A is not a decommitment corresponding to a commitment to a secret value. Gentry's public key P_A is not computed using an IBE private key. Gentry therefore fails to show or suggest using an IBE private key to compute a commitment to a secret value, as required by claim 13. Moreover, Gentry's private key is not computed using an IBE private key. Gentry therefore fails to show or suggest using an IBE private key to compute a decommitment that corresponds to a commitment to a secret value, as required by claim 13.

Deng, which was relied upon as showing using a symmetric key that is based on an IBE private key to encrypt at least one of a commitment and a decommitment, does not make up for the deficiencies of Gentry. In particular, nothing in Deng shows or suggests using an IBE private key to compute a commitment to a secret value or a corresponding decommitment. Claim 13 is therefore patentable over Gentry and Deng whether or not these references are combined as proposed in the Office Action. Claims 14-17 depend from claim 13 and are allowable because claim 13 is allowable.

Furthermore, it was conceded in the Office Action that Gentry "does not disclose using a symmetric key that is based on

the IBE private key to encrypt at least one of the commitment and the decommitment." Deng was relied upon as showing this feature.

Deng does not show or suggest using a symmetric key that is based on an IBE private key to encrypt a commitment or a decommitment. Col. 6, lines 55-57 of Deng, which was said to be relevant, describes an encrypted message " $e(k, m)$... containing original message m and a key k using a symmetric key cryptosystem." Col., 6, lines 55-57 of Deng does not relate to the commitment $h(k||I)$ of Deng. The message m and the key k of Deng, which are encrypted in col. 6, lines 55-57 of Deng, are not commitments or decommitments.

Applicant presented these arguments in the February 19, 2010 Reply. These arguments still apply and have not been addressed by the Examiner.

For at least these additional reasons, claim 13 is patentable over Gentry and Deng even if these references are combined.

Conclusion

The foregoing demonstrates that claims 1-19 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

The Commissioner is hereby authorized to charge any fees due in connection with this submission to Deposit Account No. 502942.

Respectfully submitted,

Date: August 31, 2010

/David C. Kellogg/
David C. Kellogg
Reg. No. 62,958
Telephone: 415-837-0659
Agent for Applicant
Customer No. 36532